REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
20-07-2008	Final Report	1-Jun-2007 - 29-Feb-2008

4. TITLE AND SUBTITLE

~~Secure Clustering for Wireless Sensor Networks~~

Secure and Robust Clustering in Wireless Sensor Networks

5a. CONTRACT NUMBER
W911NF-07-1-0227

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS
Donggang Liu

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of Texas at Arlington
Grants and Contracts Services
Box 19145
Arlington, TX 76019 -0145

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
52270-CI-II.4

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; Federal purpose rights

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
In many applications, sensor nodes are organized into clusters to perform efficient in-network processing (e.g., data aggregation), build scalable routing protocols, facilitate data queries, and implement efficient and scalable broadcast protocol. It is highly necessary to guarantee the trustworthiness and resilience of sensor network operations, especially when the failure of doing so

15. SUBJECT TERMS
Sensor Networks, Security, Clustering

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Donggang Liu
U	U	U	SAR		19b. TELEPHONE NUMBER 817-272-0741

Report Title

~~Secure Clustering for Wireless Sensor Networks~~ Secure and Robust Clustering in Wireless Sensor Networks

ABSTRACT

In many applications, sensor nodes are organized into clusters to perform efficient in-network processing (e.g., data aggregation), build scalable routing protocols, facilitate data queries, and implement efficient and scalable broadcast protocol. It is highly necessary to guarantee the trustworthiness and resilience of sensor network operations, especially when the failure of doing so could lead to catastrophic consequences. This project has made significant contributions to construct clusters securely and offered solutions and insights in building trustworthy sensor networks. In particular, the project has produced a secure and resilient approach for organizing initial clusters in sensor networks and a attack-resistant cluster head re-election protocol for rotating cluster heads securely in the network. In addition, the project also developed an efficient method to deal with DoS attacks against signature-based broadcast authentication. The project has supported one PhD student for 9 months.

List of papers submitted or published that acknowledge ARO support during this reporting period. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Number of Papers published in peer-reviewed journals: 0.00

(b) Papers published in non-peer-reviewed journals or in conference proceedings (N/A for none)

Number of Papers published in non peer-reviewed journals: 0.00

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts): 0

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Qi Dong, Donggang Liu, Peng Ning, Pre-Authentication Filters: Providing DoS Resistance for Signature-Based Broadcast Authentication in Wireless Sensor Networks, To appear in Proceedings of ACM Conference on Wireless Network Security (WiSec) (acceptance rate 16.7%), 2008.

Donggang Liu, Resilient Cluster Formation for Sensor Networks, in Proceedings of the International Conference on Distributed Computing Systems (ICDCS 2007) (acceptance rate 13.4%), June 2007

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts): 2

(d) Manuscripts

Qi Dong, Donggang Liu, Resilient Cluster Leader Re-Election for Sensor Networks, submitted to ICNP 2008

Number of Manuscripts: 1.00

Number of Inventions:

Graduate Students

NAME	PERCENT_SUPPORTED
Qi Dong	1.00
FTE Equivalent:	**1.00**
Total Number:	**1**

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Donggang Liu	1.00	No
FTE Equivalent:	**1.00**	
Total Number:	**1**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period:	0.00
The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:.....	0.00
The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:.....	0.00
Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):	0.00
Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:	0.00
The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense	0.00
The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:	0.00

Names of Personnel receiving masters degrees

NAME

Total Number:

Names of personnel receiving PHDs

NAME

Total Number:

Names of other research staff

NAME PERCENT_SUPPORTED

FTE Equivalent:

Total Number:

Sub Contractors (DD882)

Inventions (DD882)

Final Report for
Secure and Robust Clustering in Wireless Sensor Networks

Donggang Liu, University of Texas at Arlington

1 Introduction

A typical sensor network consists of a potentially large number of low-cost, low-power, and multi-functional sensors that communicate over short distances through wireless links [1]. Sensor networks have received a lot of attention due to their attractiveness in a variety of applications such as target tracking and data acquisition. Many protocols have been developed recently to support these applications.

Sensor nodes are often organized into clusters for efficient and scalable in-network processing (e.g, data aggregation) [13], routing [15], data query [9], and broadcast [21]. Many protocols have been developed for efficient clustering [15, 4, 3, 5, 18, 2, 6, 24]. However, they can only work in benign environments. In hostile environments, an adversary can launch many attacks against these protocols. For example, the attacker may fool the sensor nodes that are far from each other into forming a cluster or hijack the role of cluster heads by forging certain information such as the node IDs. In either case, cluster-based applications such as data aggregation may fail. This motivates the proposed research in this project.

However, protecting clustering protocols is quite challenging. First, the sensor nodes in the same cluster need to be physically close to each other in localized computations such as data aggregation. This is very difficult to guarantee in hostile environments. For example, an adversary can create wormholes [14] or invisible nodes [20] to fool the sensor nodes that are far from each other into forming a cluster. Second, sensor nodes are usually deployed in an unattended manner. An adversary can easily capture and compromise a few nodes [12]. When a sensor node is compromised, it can setup a neighbor relation with any node. An example of such an attack is the node replication attack [22] where the attacker duplicates the compromised node at many places. As a result, they can join many clusters even if authentication and encryption are employed. Another challenge is the resource constraints on sensor nodes, which makes it impractical to apply well-studied but expensive mechanisms. On the other hand, the attacker may have powerful computing devices (e.g., PDAs or Laptops) and extensive knowledge about the network.

The overall objective the proposed research is to make sure that the clusters can be formed and managed correctly in the presence of attackers. The clustering algorithms considered in this project consist of two steps, *cluster formation*, which addresses how to form initial clusters, and *cluster maintenance*, which addresses how to manage clusters such as the re-election of new cluster heads. The PI has proposed effective methods to secure both of the above two steps. Specifically, the PI has developed a *resilient cluster formation* scheme by using the neighborhood information of sensor nodes [17]. The PI has also proposed a secure and resilient method to *re-elect the cluster head* to balance the load in the cluster and prolong the cluster lifetime [7].

2 Problem Statement

This project focuses on static sensor networks where the sensor nodes do not change their locations after deployment. The network consists of the resource-constrained sensor nodes and the powerful base stations. The sensor nodes are randomly scattered to monitor the events in the field; they need to be organized into clusters to help certain network operations such as data aggregation after deployment. The base stations are used to collect/process the monitoring results or act as gateways to the traditional networks.

Attack Models: An attacker can launch many attacks against clustering. For example, he can simply perform a denial-of-service (DoS) attack to block the wireless channel. The shared channel model [10] is largely useless here since the attacker may disrespect such model. This DoS attack is simple but common to the protocols in sensor networks; there are no effective ways to stop an attacker from mounting such attack. Therefore, We strongly believe that *a security protocol would be "good enough" if the only attack impact is equivalent to blocking the channel*. Since the security of the whole system is determined by the weakest point, and an attacker can always block the channel, the "good enough" security will not reduce the security of the whole system. We thus focus on those "stealthy attacks" whose goal is to mislead the cluster formation or maintenance. We assume that an attacker can eavesdrop, modify, forge, replay and interrupt network traffic. We assume that the attacker can compromise a small number of nodes. We also assume that replicated nodes may be created and placed [22].

Design Goals for Cluster Formation: An important property for a clustering protocol is that the members of the same cluster are physically close to each other. This is critical for many applications such as data aggregation [13]. For convenience, two nodes are said to be *far away* if they do not share any actual benign neighbor. For example, if the signal range can be modeled as a circle with radius R, two nodes are far away when they are at least $2R$ meters away.

Our overall goal is to make it as difficult as possible to fool the nodes far from each other into joining the same cluster. This means that *a benign node will not join another benign node's cluster if they are far from each other, and a malicious node cannot join many clusters or recruit many benign nodes far from each other*. Note that we do not stop the attack that prevents a benign node from joining a particular cluster since this can be easily achieved by blocking the channel of the node no matter how we do.

We consider *d-hop clusters*. A node may use an intermediate node to reach the cluster head. This intermediate node is called *the uplink node*. In our technique, we have every node join the same cluster as its uplink node, which allows us to make an immediate clustering decision without the need for the decisions of other nodes. For convenience, when u uses v as its uplink node, we say "u joins the cluster *through* v " or "v *directly* recruits u".

- *Security Goal 1:* It is unlikely for a benign sensor node to select another benign sensor node (pre-determined cluster head) that is far away as its uplink node.
- *Security Goal 2:* It is difficult for a malicious node to join many clusters *through* benign sensor nodes.
- *Security Goal 3:* It is difficult for a malicious node to *directly* recruit many benign nodes far from each other.

Achieving secure clustering may reduce the performance of the protocol such as the quality of the clusters. However, in hostile environments, we believe that it is reasonable to trade off performance for security since without security, the clustering protocol will immediately fail under attacks. Although security is our number one concern, we still expect our technique to construct quality clusters (e.g., with even cluster sizes) and be efficient in terms of storage, computation and communication.

Design Goals for Cluster Head Re-Election: The objective of this step is to provide security for the election of cluster leaders in sensor networks. We identify the following security goals for a cluster leader election protocol.

- *Security Goal 1:* Unauthorized sensor nodes cannot join the cluster leader election. That is, only those legitimate members of a cluster can participate in the leader election of this cluster.
- *Security Goal 2:* The attacker cannot arbitrarily increase or decrease the chance of any benign node being elected as a cluster leader. More specifically, the attacker cannot control who will be elected as the cluster leader at any round of leader election.
- *Security Goal 3:* As long as the benign cluster members are well-connected in a particular round of leader election, they will always elect the same cluster leader for this round. This means that the result of a given round of leader election is only affected by the network connectivity during that round.

Due to node compromise, a given cluster may include a few compromised sensor nodes. It is certainly possible that a malicious sensor node is elected as the cluster leader at some point. Indeed, it is infeasible to prevent this from happening when this malicious node always acts like a normal sensor node. To mitigate such impact, one option is to ensure that every cluster member has the equal opportunity of being elected. Our protocol is designed to reinforce such fairness between cluster members. On the other hand, the compromised sensor node may start behaving maliciously once it gets elected as the new cluster leader. Detecting such misbehavior is certainly important for the security of sensor networks. However, this is beyond the scope of this project, and we consider it complementary to our approach. Nevertheless, even without such detection mechanism, our protocol can still tolerant compromised nodes in the sense that any malicious node can only serve as the cluster leader for a given period of time. The leadership will be likely shifted to a benign node in the next round of election.

3 Summary of Important Results

The PI has accomplished all the tasks identified in the proposal on time. The outcomes of these tasks are three high-quality papers. Two of them have already been published in prestigious conferences (ICDCS 2006 and WiSec 2008); the other one has been submitted for conference publication. In the following, we summarize these results.

3.1 Resilient Cluster Formation

We have developed an efficient and resilient protocol for clustering in sensor networks [17]. The main idea is to make the clustering operations *accountable*. Specifically, we propose three techniques, *simple neighbor validation*, *priority-based selection* and *centralized detection*. The simple neighbor validation provides a simple yet effective way to validate a sensor's neighbors. The priority-based selection organizes clusters based on the sensor's priority of being a cluster head and enforces the accountability of clustering decisions made by sensor nodes. The centralized detection further enhances the security of our approach by detecting misbehaving sensor nodes using the log information generated by the priority-based selection.

These three techniques result in a resilient cluster formation scheme. On the one hand, it is very difficult for an attacker to fool the benign nodes far from each other into joining the same cluster. On the other hand, a malicious node can only impact a few benign nodes; it cannot join many clusters or recruit many benign nodes far from each other in its cluster without being detected. Another appealing benefit is that a sensor node can make a clustering decision immediately once the neighborhood information (the list of neighbors) is available. This property makes it even harder to attack the cluster formation. In contrast, most existing protocols require a sensor node to wait for the decisions from many other nodes multiple hops away, introducing additional vulnerabilities.

3.2 Resilient Cluster Head Re-Election

We have proposed an efficient and resilient leader election protocol for sensor network clustering in hostile environments [7]. The security of the proposed protocol is achieved by (i) making it infeasible to forge the election values (i.e., the remaining energy) of benign sensor nodes and (ii) making the leader election protocol resistant to the malicious election values supplied by compromised sensor nodes. Similar to most existing cluster leader election protocols, we use the remaining energy on sensor nodes as the metric to determine the cluster leader. However, our approach is also different from them in that we do not use the one with the most remaining energy as the new cluster leader. Instead, the role of cluster leader will be rotated among all cluster members that are qualified for being elected as the cluster leader, i.e., those nodes whose energy is greater than a pre-determined system threshold E_{th}, which is the minimum energy required for serving as the cluster leader. This will make it very difficult for any malicious insider to hijack the role of cluster leader frequently by forging the election value.

The proposed scheme has several nice properties. First, it guarantees that the benign cluster members in a given cluster will agree on the same cluster leader as long as they are well-connected. Second, an attacker cannot impact the leader election protocol to increase or decrease the chance of a benign sensor node being elected as the cluster leader. Third, it tolerates message loss effectively. The leader election can recover quickly from failures once the network in the local area becomes well-connected again. This important property makes it difficult for adversaries to disrupt the leader election by jamming the communication channel for only a short period of time. A long-term jamming attack is still very expensive and can be easily detected to physically locate the adversary. Finally, the proposed scheme is fully distributed. This addresses the problem of the single point of failure.

3.3 Pre-Authentication Filters

We have proposed to apply *pre-authentication filters* to remove bogus messages before the actual signature verification is performed [8]. This scheme can be used to address the message authentication problem in the previous two approaches. Indeed, these pre-authentication filters are developed when we were trying to find suitable broadcast authentication methods in previous research tasks.

Initially, we believe that ECC-based signature schemes will be an attractive option for broadcast authentication in many applications. Indeed, recent studies have demonstrated that it is possible to perform public key cryptographic operations on resource-constrained sensor platforms [11]. In addition, there have been continuous efforts to optimize Elliptic Curve Cryptography (ECC) for sensor platforms [16, 23, 19]. However, the significant resource consumption imposed by public key cryptographic operations makes such mechanisms easy targets of Denial-of-Service (DoS) attacks. For example, if ECDSA is used directly for broadcast authentication without further protection, an attacker can simply broadcast forged packets and force the receiving nodes to perform a large number of unnecessary signature verifications, eventually exhausting their battery power. To address the above problem, we developed two filtering techniques, a *group-based filter* and a *key chain-based filter*, to help sensor nodes avoid performing many unnecessary signature verifications. Both methods take advantage of the fact that broadcast in sensor networks is usually done through a network-wide flooding protocol, and a broadcast message from a sensor node usually has a small number of immediate receivers due to the low-power, short-range radio used in wireless sensor networks.

The proposed pre-authentication filters provide complementary capabilities in dealing with DoS attacks against signature-based broadcast authentication. The group-based filter organizes the neighbor nodes of a (local) sender into multiple groups, which are protected by different keys organized in a tree structure. Using these group keys, this mechanism not only facilitates the neighbor nodes to filter out forged messages, but also helps the sender adaptively isolate compromised nodes that launch DoS attacks. Unfortunately, the group-based filter allows compromised nodes to send forged messages before they are isolated. The key chain-based filter employs a *two-layer* method, completely preventing compromised neighbor nodes from affecting benign ones. The first layer uses one-way key chains to mitigate the DoS attacks against signature verification, and the second layer uses pairwise keys to mitigate the DoS attacks on the verification of the chained keys in the first layer. However, despite the advantage in tolerating compromised nodes, the key chain-based filter defers to the group-based filter in the ability to tolerate packet losses.

4 Conclusion

The PI has successfully accomplished the research tasks identified in this project. Three novel techniques are produced from this project. First, we propose an efficient and effective technique for *resilient cluster formation*, which consists of a simple neighbor validation, a priority-based selection and a centralized detection. The proposed neighbor validation is of independent interest; it can further improve the security of current wormhole detector. Sec-

ond, we present an *efficient and resilient cluster leader election* protocol for sensor networks. It is very difficult for an adversary to disrupt the protocol without launching intensive channel jamming attacks for a long time period or compromising a large number of cluster members. This protocol is also resistant to message loss; it can quickly recover from any failure as long as the benign cluster members are well-connected during the time of recovery. Third, we propose two *pre-authentication filters*, a group-based method and a key chain-based method, to effectively mitigate the DoS attacks against the signature verification in broadcast authentication. Our analysis and simulation studies indicate that the proposed protocols are efficient and effective in dealing with malicious attacks.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: A survey. *Computer Networks*, 38(4):393–422, 2002.

[2] A.D. Amis, R. Prakash, T.H.P. Vuong, and D. T. Huynh. Max-min d-cluster formation in wireless ad hoc networks. In *Proceedings of IEEE INFOCOM 2002*, March 1999.

[3] D.J. Baker, A. Ephremides, and J.A. Flynn. The design and simulation of a mobile radio networkwith distributed control. *IEEE*, SAC-2(1):226–237, 1984.

[4] S. Banerjee and S. Khuller. A clustering scheme for hierarchical control in wireless networks. In *Proceedings of IEEE INFOCOM 2001*, 2001.

[5] S. Basagni. Distributed clustering for ad hoc networks. In *Proceedings of the 1999 International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN '99)*, 1999.

[6] H. Chan and A. Perrig. ACE: An emergent algorithm for highly uniform cluster formation. In *European Workshop on Wireless Sensor Networks (EWSN 2004)*, Jan 2004.

[7] Q. Dong and D. Liu. Resilient cluster leader election for wireless sensor networks. Submitted for conference publication, 2008.

[8] Q. Dong, D. Liu, and P. Ning. Pre-authentication filters: Providing dos resistance for signature-based broadcast authentication in wireless sensor networks. In *Proceedings of ACM Conference on Wireless Network Security (WiSec)*, 2008.

[9] D. Estrin, R. Govindan, J. S. Heidemann, and S. Kumar. Next century challenges: Scalable coordination in sensor networks. In *Proceedings of ACM MobiCom 1999*, 1999.

[10] C. A. Gunter, S. Khanna, K. Tan, and S. Venkatesh. Dos protection for reliably authenticated broadcast. In *Proceedings of the Network and Distributed System Security (NDSS'04*, Feb 2004.

[11] N. Gura, A. Patel, and A. Wander. Comparing elliptic curve cryptography and rsa on 8-bit CPUs. In *Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, August 2004.

[12] C. Hartung, J. Balasalle, and R. Han. Node compromise in sensor networks: The need for secure systems. Technical Report CU-CS-990-05, U. Colorado at Boulder, Jan. 2005.

[13] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In *Proceedings of the Hawaii International Conference on System Sciences HICSS*, 2000.

[14] Y.C. Hu, A. Perrig, and D.B. Johnson. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In *Proceedings of INFOCOM*, April 2003.

[15] P. Krishna, N. H. Vaidya, M. Chatterjee, and D. K. Pradhan. A cluster-based approach for routing in dynamic networks. *SIGCOMM Computer Communication Review*, 27(2), 1997.

[16] A. Liu and P. Ning. TinyECC: Elliptic curve cryptography for sensor networks. `http://discovery.csc.ncsu.edu/software/TinyECC/index.html`.

[17] D. Liu. Resilient cluster formation for sensor networks. In *Proceedings of the International Conference on Distributed Computing Systems (ICDCS)*, June 2007.

[18] S.K. Das M. Chatterjee and D. Turgut. Wca: A weighted clustering algorithm for mobile ad hoc networks. *Journal of Cluster Computing (Special Issue on Mobile Ad hoc Networks)*, 5(2):193–204, 2002.

[19] D. J. Malan, M. Welsh, and M. D. Smith. A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography. In *Proceedings of First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (IEEE SECON 2004)*, pages 71–80, 2004.

[20] J. Marshall. An analysis of srp for mobile ad hoc networks. In *Proceedings of the 2002 International Multiconference in Computer Science*, August 2002.

[21] E. Pagani and G.P. Rossi. Reliable broadcast in mobile multihop packet networks. In *Proceedings of MobiCom' 97*, 1997.

[22] B. Parno, A. Perrig, and V. Gligor. Distributed detection of node replication attacks in sensor networks. In *IEEE Symposium on Security and Privacy*, May 2005.

[23] H. Wang, B. Sheng, C. C. Tan, and Q. Li. WM-ECC: an Elliptic Curve Cryptography Suite on Sensor Motes. Technical Report WM-CS-2007-11, College of William and Mary, Computer Science, Williamsburg, VA, 2007.

[24] O. Younis and S. Fahmy. Distributed clustering in ad-hoc sensor networks: A hybrid, energy-efficient approach. In *Proceedings of IEEE INFOCOM 2004*, March 2004.